Załącznik nr 5 do Polityki ochrony danych osobowych

INSTRUKCJA
zarządzania systemem informatycznym (IZSI)
służącym do przetwarzania danych osobowych

u przedsiębiorcy – Moniki Michalak, prowadzącej działalność gospodarczą pod nazwą: BABY-HOUSE ŻŁOBEK KLUB MALUCHA MONIKA MICHALAK, Zakrzewo, ul. Gajowa 66, 62-070 Dopiewo, NIP: 7772424028, REGON: 300384698, zwanej dalej: „Przedsiębiorcą" lub „BABY-HOUSE";

IZSI została zatwierdzona przez administratora danych osobowych w dniu 09 lipca 2018 r.

IZSI została wprowadzona w życie z dniem 09 lipca 2018 r.

WPROWADZENIE

1. Niniejszy dokument stanowi Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych u przedsiębiorcy – **Moniki Michalak, prowadzącej działalność gospodarczą pod nazwą: BABY-HOUSE ŻŁOBEK KLUB MALUCHA MONIKA MICHALAK, Zakrzewo, ul. Gajowa 66, 62-070 Dopiewo, NIP: 7772424028, REGON: 300384698**, zwany dalej „Instrukcją" i jest wypełnieniem obowiązku wynikającego z art. 24 ust. 1 i ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych lub RODO).

2. Instrukcja określa sposób zarządzania systemem informatycznym, wykorzystywanym do przetwarzania danych osobowych, w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

3. W Instrukcji zostały uregulowane procedury:

1) nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych oraz wskazanie osób odpowiedzialnych za te czynności;
2) rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
3) tworzenia kopii zapasowych zbiorów danych oraz określenie programów i narzędzi programowych służących do ich przetwarzania wraz z określeniem sposobu, miejscem i okresem ich przechowywania;
4) wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych;
5) metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
6) sposoby zabezpieczenia systemu informatycznego przed działalnością oprogramowania szkodliwego oraz dostępem do nich osób nieupoważnionych.

POSTANOWIENIA OGÓLNE

A. Słownik pojęć użytych w Instrukcji

Użyte w Instrukcji określenia oznaczają:

1) administrator danych osobowych - **Monika Michalak, prowadząca działalność gospodarczą pod nazwą: BABY-HOUSE ŻŁOBEK KLUB MALUCHA MONIKA MICHALAK**, decydujący o celach i środkach przetwarzania danych osobowych, odpowiedzialny za nadzór nad przestrzeganiem zasad ochrony danych

osobowych w jednostce oraz wykonujący zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym, zwany dalej ADO;

2) bezpieczeństwo informacji - stan, w którym informacja jest chroniona przed wieloma różnymi zagrożeniami w taki sposób, aby zapewnić ciągłość prowadzenia działalności, zminimalizować straty i maksymalizować zwrot nakładów na inwestycje i działania o charakterze biznesowym; niezależnie od tego, jaką formę informacja przybiera lub za pomocą jakich środków jest udostępniana lub przechowywana, zawsze powinna być w odpowiedni sposób chroniona; bezpieczeństwo informacji oznacza w szczególności zachowanie: poufności, integralności, dostępności i rozliczalności;
3) dane osobowe (dane) - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
4) hasło - ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;
5) identyfikator - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
6) integralność danych - właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
7) IZSI - niniejsza Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej Instrukcją;
8) kopia bezpieczeństwa - kopie plików danych lub plików programowania tworzone na nośnikach wymiennych lub dysku twardym komputera w celu ich odtworzenia w przypadku utraty lub uszkodzenia danych;
9) odbiorca danych - każdy, komu udostępniane są dane osobowe, z wyłączeniem:
   a) osoby, której dane dotyczą,
   b) osoby upoważnionej do przetwarzania danych,
   c) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;
10) osoba upoważniona do przetwarzania danych osobowych - osoba, która upoważniona została do przetwarzania danych osobowych przez ADO na piśmie;
11) poufność danych - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;
12) proces zarządzania bezpieczeństwem systemów informatycznych - całość działań organizacyjno-technicznych i prawnych podejmowanych przez jednostkę mających na celu właściwą ochronę informacji oraz minimalizację skutków w przypadku incydentów bezpieczeństwa;
13) przetwarzanie danych - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
14) przetwarzający dane - podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy, zgodnie z art. 28 RODO;
15) raport - przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
16) serwisant - firma lub pracownik firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego;
17) system informatyczny (system) - sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną ADO;
18) system zarządzania bezpieczeństwem informacji - całościowy i uporządkowany układ, który tworzą następujące procedury i procesy:
   a) ustanowienie polityki bezpieczeństwa informacji – Polityki ochrony danych osobowych,
   b) określenie zakresu zarządzania bezpieczeństwem informacji,
   c) ocena zagrożeń bezpieczeństwa informacji i zarządzanie ryzykiem związanym z zagrożeniami,
   d) wprowadzenie standardów bezpieczeństwa informacyjnego,
   e) opracowanie planu ciągłości działania,
   f) edukacja pracowników w zakresie bezpieczeństwa informacji;

19) trwałe usunięcie informacji - sposób postępowania z nośnikiem informacji mający na celu usunięcie zapisanych na nim informacji tak, aby ich odtworzenie w całości lub w części było niemożliwe;
20) ustawa - rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych;
21) uwierzytelnianie - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
22) użytkownik - osoba upoważniona do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło;
23) zagrożenie - stan faktyczny, który może spowodować naruszenie bezpieczeństwa informacji;
24) zasada wiedzy koniecznej - oznacza, że dostęp osób zatrudnionych w jednostce do zasobów informacyjnych ograniczony jest wyłącznie do informacji, które są im niezbędne do wykonania powierzonych zadań;
25) RODO - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

B. Zakres przedmiotowy Instrukcji

1. Instrukcja ma zastosowanie do każdego zbioru danych osobowych:
1) przetwarzanych w systemach informatycznych w jednostce,
2) zapisanych w formie elektronicznej na zewnętrznych nośnikach.

C. Zakres podmiotowy Instrukcji

1. Do stosowania postanowień Instrukcji obowiązani są wszyscy pracownicy jak i inne osoby, które przetwarzają dane osobowe w systemach informatycznych jednostki.

2. Przed przystąpieniem do pracy przez pracownika lub innej osoby zatrudnionej w jednostce obowiązkowe jest zapoznanie się z regulacjami dotyczącymi przetwarzania danych w jednostce, w szczególności z:
1) Polityką ochrony danych osobowych, zwanej dalej: „Polityką”;
2) Instrukcją zarządzania systemem informatycznym dla jednostki.

3. Fakt zapoznania się z regulacjami, o których mowa w pkt 2, potwierdzany jest poprzez podpisanie oświadczenia o zachowaniu poufności informacji uzyskiwanych w związku z przetwarzaniem danych osobowych oraz zapoznaniu się z zasadami przetwarzania danych.

4. Oświadczenie, o którym mowa w pkt 3, stanowi załącznik nr 6 do Polityki.

D. System informatyczny

1. Na System informatyczny w jednostce składają się:
1) urządzenia:
   a) komputer użytkowany przez administratora danych osobowych,
   b) telefon użytkowany przez administratora danych osobowych,
2) programy: systemy operacyjne zainstalowane na urządzeniach wymienionych powyżej;

2. Elementy Systemu opisane w ust. 1 są wykorzystywane do przetwarzania danych w jednostce. Podlegają one regularnej kontroli w celu zapewnienia bezpieczeństwa przetwarzanych danych.

E. Klasyfikacja systemów informatycznych

1. Każdy system informatyczny eksploatowany w jednostce wymaga zaklasyfikowania do określonej kategorii ze względu na poziom poufności, integralności i dostępności przetwarzanych informacji oraz na rodzaj informacji i wagę systemu dla ciągłości świadczenia usług.

2. Poziom wymagań odnośnie bezpieczeństwa przetwarzanych informacji wyznaczają przepisy prawa oraz wymagania ekonomiczne określane każdorazowo przez ADO.

3. Systemy informatyczne eksploatowane w jednostce kategoryzuje i opisuje IZSI.

4. Za sklasyfikowanie systemów informatycznych eksploatowanych w jednostce odpowiada ADO. Klasyfikacja systemów informatycznych podlega akceptacji ADO.

ZARZĄDZANIE DOSTĘPEM I BEZPIECZEŃSTWEM SYSTEMÓW

A. Zarządzanie dostępem

1. Dostęp do systemów informatycznych musi być zabezpieczony z wykorzystaniem obowiązujących w jednostce mechanizmów bezpieczeństwa w postaci rozwiązań organizacyjno-technicznych i prawnych uwzględniających kategorię systemu oraz wrażliwość informacji przetwarzanych w systemie.

2. Mechanizmy bezpieczeństwa muszą zapewniać rozliczalność w stopniu uwzględniającym kategorię systemu oraz wymagania wynikające z przepisów prawa i przepisów wewnętrznych jednostki. W szczególności każdemu użytkownikowi systemu informatycznego musi być przydzielony niepowtarzalny identyfikator.

3. Każdy użytkownik systemu informatycznego zobowiązany jest do eksploatowania systemów informatycznych zgodnie z procedurami opisanymi w IZSI.

4. Dostęp do zasobów informatycznych oraz działania wykonywane z kont użytkowników, kont administratorów systemu, muszą być monitorowane w stopniu uwzględniającym poziom uprawnień przypisany do tych kont oraz kategorię systemu.

5. Monitoringowi podlegają w szczególności działania, których wykonanie jest krytyczne dla bezpieczeństwa systemu i bezpieczeństwa przetwarzanych informacji.

6. Osoba pełniąca funkcję administratora systemu powinna posiadać dodatkowo odrębne konto służące tylko i wyłącznie do administracji danym systemem informatycznym o ile dany system udostępnia taką funkcjonalność.

7. Dostęp do systemów informatycznych wygasa:

1) zgodnie z zasadą wiedzy koniecznej,
2) po upływie okresu, na który został przyznany,
3) w przypadku zawinionego naruszenia bezpieczeństwa systemu lub bezpieczeństwa przetwarzanych danych.

8. Zasady fizycznego dostępu do pomieszczeń, w których zlokalizowane są zasoby informatyczne, określa IZSI.

9. Zasady szczegółowe:

1) poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania;
2) ADO przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem;
3) w razie potrzeby ADO może przydzielić konto opatrzone identyfikatorem osobie upoważnionej do przetwarzania danych osobowych, nieposiadającej statusu pracownika;
4) pierwsze hasło wymagane do uwierzytelnienia się w systemie przydzielane jest przez ADO po odebraniu od osoby upoważnionej do przetwarzania danych oświadczenia zawierającego zobowiązanie do zachowania w tajemnicy pierwszego i następnych haseł oraz potwierdzenie odbioru pierwszego hasła;
5) do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji.

B. Analiza i zarządzanie ryzykiem

1. Podstawowe zagrożenia dla poprawnego funkcjonowania systemów informatycznych mogą wynikać z awaryjności sprzętu komputerowego, oprogramowania, czynnika ludzkiego oraz zdarzeń losowych.

2. Skutkiem wystąpienia zagrożenia zasobów informatycznych może być:

1) zniszczenie części lub całości systemu informatycznego,
2) utrata danych,
3) utrata poufności, integralności, dostępności, rozliczalności lub autentyczności danych,
4) straty finansowe,
5) utrata wiarygodności i dobrego wizerunku.

3. Za proces analizy i zarządzania ryzykiem odpowiedzialny jest ADO.

4. Proces analizy ryzyka obejmuje analizę zagrożeń, analizę podatności, analizę skutków wystąpienia zagrożeń oraz analizę istniejących zabezpieczeń i jest realizowany w ramach procesu samooceny ryzyka w jednostce.

5. Wyniki analizy ryzyka stanowią podstawę wyboru odpowiednich zabezpieczeń dla systemów

informatycznych eksploatowanych w jednostce.

6. Wdrażane zabezpieczenia powinny zapewniać efektywność ekonomiczną oraz skutkować akceptowalnym ryzykiem szczątkowym.

7. Kryteria akceptowalności ryzyka szczątkowego wdrażanych zabezpieczeń powinny stanowić pisemne załączniki do dokumentacji wdrażanych zabezpieczeń.

C. Cele i zasady bezpieczeństwa systemu

1. Stosowanie zabezpieczeń ma na celu zapewnienie optymalnego poziomu bezpieczeństwa przetwarzanych w systemie danych, stosownie do ich rodzaju oraz ewentualnych zagrożeń.

2. Zapewnienie odpowiedniego poziomu bezpieczeństwa następuje poprzez stosowanie zasad, zgodnie z którymi:

1) osoby nieupoważnione nie mają dostępu do systemu;
2) użytkownicy mają ograniczony dostęp do systemu, zgodnie z postanowieniami niniejszej Instrukcji;
3) użytkownicy wykorzystują oddane im do dyspozycji narzędzia zgodnie z zaleceniami, zachowując wymogi należytej staranności.

D. Poziom bezpieczeństwa

1. Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym połączonym z siecią publiczną, wprowadza się "poziom wysoki" bezpieczeństwa.

2. Zastosowanymi środkami bezpieczeństwa są:

1) środki ochrony organizacyjne,
2) środki ochrony fizyczne,
3) środki ochrony techniczne.

E. Nadawanie uprawnień w systemach informatycznych

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych zarejestrowana jako użytkownik w tym systemie przez ADO.

2. W jednostce przetwarzać dane mogą jedynie osoby posiadające ww. upoważnienie, które złożyły oświadczenia o zachowaniu poufności przetwarzanych danych oraz odbyły obowiązkowe szkolenie z zakresu ochrony danych osobowych.

3. ADO jest obowiązany upoważnić co najmniej jednego pracownika do rejestracji użytkowników w systemie informatycznym w czasie swojej nieobecności dłuższej niż 14 dni.

4. ADO prowadzi wykaz osób dopuszczonych do przetwarzania danych osobowych.

5. Rejestr osób upoważnionych do przetwarzania danych osobowych, o którym mowa w pkt 4 stanowi załącznik nr 4 do Polityki.

6. Rejestracja użytkownika polega na nadaniu identyfikatora i przydzieleniu hasła, zakresu przetwarzania danych oraz wprowadzeniu tych danych do bazy użytkowników systemu.

7. Konto użytkownika na serwerze/dysku zakłada ADO, na podstawie upoważnienia do przetwarzania danych osobowych, nadając unikalną nazwę użytkownika i hasło.

8. Przydzielone użytkownikowi hasło przekazywane jest w formie ustnej, ulega zmianie przez użytkownika po pierwszym zalogowaniu się do systemu.

9. Użytkownik obowiązany jest do zachowania w tajemnicy hasła, w szczególności nieudostępniania go innym użytkownikom, niezapisywania w powszechnie dostępnych miejscach.

10. Upoważnienie do przetwarzania danych osobowych w systemach informatycznych nadawane jest na określony czas, który nie może przekroczyć okresu stosunku zatrudnienia osoby będącej użytkownikiem.

11. W przypadku przedłużenia upoważnienia do przetwarzania danych, przedłużeniu na taki sam czas ulega ważność konta dostępu użytkownika.

F. Usunięcie konta

1. Usuwanie kont z systemu informatycznego dokonywane jest przez ADO.

2. Usunięcie konta następuje w przypadku:

1) rozwiązania stosunku pracy;
2) wygaśnięcia stosunku pracy;
3) ustania innego stosunku prawnego, w ramach którego zatrudniony był użytkownik;
4) przejścia użytkownika do innej jednostki organizacyjnej;
5) cofnięcia upoważnienia do przetwarzania danych osobowych.

3. Usunięcie konta ma charakter definitywny, co oznacza, że niedopuszczalne jest jego ponowne wykorzystywanie przez tego samego albo innego użytkownika.

G. Wyrejestrowanie użytkownika

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje ADO.
2. Wyrejestrowanie, o którym mowa w pkt 1, ma charakter czasowy.
3. Wyrejestrowanie następuje poprzez zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę.
4. Czasowe wyrejestrowanie użytkownika z systemu informatycznego musi nastąpić w razie:
1) nieobecności użytkownika w pracy trwającej dłużej niż 30 dni kalendarzowych;
2) zawieszenia w pełnieniu obowiązków służbowych.
5. Przyczyną wyrejestrowania użytkownika z systemu informatycznego jest w szczególności:
1) wypowiedzenie umowy o pracy;
2) wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych.

H. Użytkownik uprzywilejowany

1. ADO jest użytkownikiem uprzywilejowanym, posiadającym najwyższe uprawnienia w systemie informatycznym.
2. Konto użytkownika uprzywilejowanego jest używane tylko w uzasadnionych przypadkach.
3. Hasło ADO jest przechowywane w siedzibie ADO i jest odpowiednio zabezpieczone.

I. Kontrola bezpieczeństwa

1. Codzienna kontrola bezpieczeństwa jest wykonywana przez użytkowników i polega w szczególności na sprawdzeniu, czy nie doszło do:
1) próby nieautoryzowanego dostępu do systemu;
2) próby nieautoryzowanej zmiany oprogramowania;
3) próby nieautoryzowanej modyfikacji danych;
4) ujawnienia lub udostępnienia innym osobom nazwy lub hasła;
5) uszkodzenia lub zniszczenia urządzeń systemu.
2. W razie stwierdzenia nieprawidłowości w zakresie bezpieczeństwa użytkownik powiadamia niezwłocznie ADO.
3. Okresowa kontrola bezpieczeństwa jest wykonywana przez ADO.

UTRZYMANIE, ROZWÓJ I WYCOFANIE SYSTEMÓW INFORMATYCZNYCH

A. Rozwój systemów informatycznych

1. Rozwój systemów informatycznych dotyczy wdrożenia nowych lub modernizacji aktualnie eksploatowanych systemów informatycznych, a w szczególności zmiany architektury systemów lub ich funkcjonalności.
2. Rozwój systemów informatycznych obejmuje w szczególności następujące działania:
1) określenie kategorii systemu informatycznego;
2) analizę wymagań biznesowych;
3) analizę ryzyk związanych z wdrożeniem nowego systemu informatycznego lub jego modernizacji, projektowanie architektury i funkcjonalności systemów informatycznych z uwzględnieniem aspektów bezpieczeństwa;
4) implementację mechanizmów bezpieczeństwa zgodnych z wymaganiami biznesowymi;
5) testowanie systemu informatycznego przed jego wdrożeniem do eksploatacji;

6) opracowanie dokumentacji bezpieczeństwa dla systemu informatycznego;
7) przeszkolenie użytkowników systemu informatycznego.

3. Za rozwój systemów informatycznych w jednostce odpowiada ADO.

4. Testowanie systemów informatycznych powinno odbywać się wyłącznie z wykorzystaniem danych testowych w odseparowanym środowisku.

5. Rozpoczęcie eksploatacji systemu informatycznego wymaga decyzji ADO.

6. ADO sprawuje nadzór merytoryczny nad wdrożeniem mechanizmów bezpieczeństwa właściwych dla kategorii systemu informatycznego.

B. Utrzymanie systemów informatycznych

1. Utrzymanie systemów informatycznych obejmuje następujące działania:
1) analizę ryzyka związanego z funkcjonowaniem systemu informatycznego;
2) instalację, konfigurację, serwisowanie oraz administrację zasobami sprzętowymi i oprogramowaniem wchodzącym w skład systemu informatycznego z uwzględnieniem aspektów bezpieczeństwa.

2. Eksploatacja systemów informatycznych obejmuje działania związane z:
1) użytkowaniem systemu,
2) okresowym testowaniem i kontrolą zaimplementowanych mechanizmów bezpieczeństwa oraz odpowiednim dokumentowaniem tych działań.

3. Za utrzymanie systemów informatycznych odpowiada ADO.

4. ADO sprawuje nadzór merytoryczny nad eksploatacją i utrzymaniem właściwych mechanizmów bezpieczeństwa wszystkich systemów informatycznych eksploatowanych w jednostce.

C. Wycofanie systemów informatycznych

1. Systemy informatyczne, nośniki informacji lub inne zasoby informacyjne, które przestały być używane, wycofuje się z eksploatacji w sposób opisany w IZSI.

2. Wycofanie systemu informatycznego z eksploatacji wymaga przestrzegania właściwych procedur bezpieczeństwa obejmujących w szczególności zasady postępowania:
1) z informacją przetwarzaną w systemie informatycznym i nośnikami informacji,
2) z dokumentacją bezpieczeństwa zasobu informatycznego.

METODY I ŚRODKI UWIERZYTELNIANIA

A. Nazwa i hasło użytkownika

1. Uwierzytelnienie użytkownika w Systemie Informatycznym następuje po podaniu nazwy użytkownika i hasła.

2. Nazwa użytkownika stanowi identyfikator, który w sposób jednoznaczny przypisany został konkretnemu użytkownikowi.

3. Identyfikator składa się z ciągu przynajmniej ośmiu znaków.

4. Niedopuszczalne jest funkcjonowanie kilku takich samych nazw użytkowników. Raz przypisana nazwa nie podlega zmianie i nie może zostać wykorzystana w przyszłości przez innego użytkownika.

5. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika ADO nadaje inny identyfikator, odstępując od zasady określonej w pkt 4.

6. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

7. Hasło nie może być:
1) identyczne z identyfikatorem użytkownika;
2) identyczne z imieniem lub nazwiskiem użytkownika;
3) odnosić się do innych cech szczególnych użytkownika;
4) ponowieniem hasła stosowanego wcześniej, jeżeli od ostatniego zastosowania danej kombinacji nie upłynął rok.

8. Niedopuszczalne jest zapamiętywanie haseł w systemie.

9. Pierwsze nadane hasło ulega zmianie przez użytkownika.

10. W przypadku, gdy system umożliwia limitowanie wprowadzenia błędnego hasła, należy przyjąć próg ilości wprowadzonych błędnych haseł na 3/5. Po przekroczeniu limitu powinna nastąpić automatyczna blokada

konta.

11. Użytkownik odpowiada za działania wykonywane w systemie przy użyciu jego nazwy oraz za zachowanie hasła w tajemnicy.

12. Użytkownik ma obowiązek zmieniać hasło nie rzadziej niż co 90 dni.

13. Okresowe zmiany hasła są wykonywane osobiście przez użytkownika.

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM

A. Zasady korzystania ze stacji roboczej/komputerów przenośnych

1. Przed rozpoczęciem pracy użytkownik obowiązany jest sprawdzić stan urządzeń oraz dokonać oględzin swojego stanowiska pracy w celu wykrycia ewentualnych nieprawidłowości mogących świadczyć o naruszeniu bezpieczeństwa danych osobowych.

2. W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika lub ADO.

3. Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać podgląd), a także wydruki leżące na biurkach oraz w otwartych szafach.

4. Rozpoczęcie pracy:

1) włączenie napięcia w listwie podtrzymującej napięcie,
2) włączenie monitora i stacji roboczej,
3) zalogowanie się poprzez wprowadzenie nazwy użytkownika i hasła,
4) uruchomienie programu użytkowego.

5. Zawieszenie pracy w przypadku czasowego opuszczenia stanowiska pracy:

1) zablokowanie sesji na stacji roboczej,
2) odblokowanie sesji po podaniu hasła.

6. W przypadku bezczynności na stacji roboczej przez czas przekraczający 2 minuty automatycznie włącza się wygaszacz ekranu, który powinien być zaopatrzony w hasło umożliwiające ponowne podjęcie pracy na stacji roboczej.

7. Zakończenie pracy:

1) zakończenie pracy programu zgodnie z instrukcją obsługi,
2) wylogowanie z systemu,
3) wyłączenie stacji roboczej i monitora,
4) wyłączenie napięcia w listwie podtrzymującej napięcie.

8. Krótkotrwała przerwa w pracy, podczas której użytkownik nie opuszcza stanowiska roboczego, nie wymaga zamykania aplikacji, wylogowania.

9. Każdorazowa zmiana użytkownika stacji roboczej musi poprzedzać wylogowanie się użytkownika, który poprzednio z niej korzystał.

10. Procedury określone w niniejszej Instrukcji, dotyczące pracy na komputerach stacjonarnych mają odpowiednie zastosowanie przy przetwarzaniu danych osobowych na komputerach przenośnych.

SPOSOBY ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO

A. Ochrona antywirusowa

1. W jednostce istnieje bezwzględny wymóg instalacji oprogramowania antywirusowego na każdym stanowisku roboczym, zarówno na komputerach stacjonarnych, jak i przenośnych wykorzystywanych do przetwarzania danych.

2. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach/dyskach, stacjach roboczych oraz komputerach przenośnych przez ADO.

3. Oprogramowanie, o którym mowa w ust. 2, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami/dyskami i stacjami roboczymi.

4. Niezależnie od ciągłego nadzoru, o którym mowa w ust. 3, ADO nie rzadziej niż raz na 3 miesiące przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach/na dyskach i stacjach roboczych.

5. Niedopuszczalne jest wyłączanie lub zmiana ustawień oprogramowania antywirusowego przez

użytkowników.

6. Użytkownik jest obowiązany zawiadomić ADO o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.

7. Do obowiązków ADO należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez to oprogramowanie.

8. ADO przeprowadza cyklicznie kontrole antywirusowe na każdym stanowisku komputerowym wykorzystywanym do przetwarzania danych, w tym na komputerach przenośnych.

9. Użytkownicy mogą korzystać z zewnętrznych nośników danych tylko na stanowisku wydzielonym z sieci komputerowej ADO po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.

10. Niedopuszczalne jest otwieranie plików pobranych z Internetu lub korzystania z zewnętrznych nośników bez uprzedniego przeskanowania zawartości nośnika przez program antywirusowy.

11. Przesyłanie danych osobowych pocztą elektroniczną dopuszczalne jest tylko w postaci zaszyfrowanej.

B. Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych

1. System informatyczny umożliwia automatycznie:

1) przypisanie wprowadzanych danych użytkownikowi (identyfikatorowi użytkownika), który te dane wprowadza do systemu;
2) sygnalizację wygaśnięcia czasu obowiązywania hasła dostępu do stacji roboczej (dotyczy to także komputerów przenośnych);
3) sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w systemie, raportu zawierającego:
   a) datę pierwszego wprowadzenia danych do systemu administratora danych,
   b) identyfikator użytkownika wprowadzającego te dane,
   c) źródła danych - w przypadku zbierania danych nie od osoby, której one dotyczą,
   d) informacje o odbiorcach danych, którym dane osobowe zostały udostępnione.

2. Odnotowanie informacji, o których mowa w pkt 3, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Rejestr uwzględniający elementy, o których mowa w pkt 1, prowadzony jest przez ADO w formie elektronicznej/papierowej.

4. Nadzór nad prawidłowym wprowadzaniem, przetwarzaniem i udostępnianiem danych sprawuje ADO.

5. Nadzór wykonywany jest w sposób niezapowiedziany lub zapowiedziany z jednodniowym wyprzedzeniem. Ponadto czynności kontrolne przeprowadzane są obligatoryjnie w przypadku uzasadnionego podejrzenia / naruszenia bezpieczeństwa Systemu.

6. Nadzór, o którym mowa obejmuje m.in.:

1) sprawdzenie, czy przetwarzanie danych w Systemie odbywa się z poszanowaniem zasad uregulowanych w niniejszej IZSI;
2) sprawdzanie zabezpieczeń stosowanych przez jednostkę, mających na celu zapewnienie ochrony danych, w tym zabezpieczeń fizycznych, organizacyjnych oraz technicznych;
3) kontrolę rejestru udostępnień danych;
4) oględziny urządzeń służących do przetwarzania danych, m.in.: serwery/dyski, stacje robocze.

C. Bezpieczeństwo oprogramowania

1. Oprogramowanie stosowane w jednostce może pochodzić wyłącznie ze źródeł legalnych oraz posiadać aktualną i kompletną dokumentację użytkownika, eksploatacyjną i techniczną, a w przypadku gdy przy jego pomocy przetwarzane są dane osobowe - zgodną z RODO.

2. Instalacja i deinstalacja dokonywana jest wyłącznie przez ADO.

3. Użytkownicy obowiązani są do powstrzymania się od jakiejkolwiek ingerencji w oprogramowanie.

4. Wszelkie oprogramowanie wykorzystywane w jednostce musi być użytkowane z poszanowaniem praw własności intelektualnej, a w szczególności zgodnie z ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych.

5. Za określanie oraz zmiany w obowiązujących standardach sprzętu i oprogramowania odpowiada ADO. Standard sprzętu i oprogramowania powinien być zgodny z wymaganiami biznesowymi, uwzględniać opłacalność ekonomiczną oraz wymagania w zakresie bezpieczeństwa.

Sprzęt i oprogramowanie powinny być eksploatowane, serwisowane i wycofywane z eksploatacji z zachowaniem właściwych procedur bezpieczeństwa.

6. Wszelkie działania związane z utrzymaniem i eksploatacją systemu informatycznego mogą być podejmowane wyłącznie przez upoważniony, wykwalifikowany personel jednostki lub upoważnione osoby.

WYKONYWANIE PRZEGLĄDÓW, KONSERWACJI ORAZ NAPRAW URZĄDZEŃ SYSTEMU ORAZ NOŚNIKÓW

A. Procedura wykonywania przeglądów i konserwacji urządzeń

1. Przegląd i konserwacja urządzeń systemu winna być dokonywana zgodnie z zaleceniami producenta, nie rzadziej niż co 12 miesięcy.
2. Przeglądu i konserwacji systemu dokonuje doraźnie ADO, który odpowiedzialny jest za terminowość i rzetelność przeglądów i konserwacji urządzeń.
3. Wszelkie nieprawidłowości wykryte w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny oraz okoliczności sprzyjające przeanalizowane. O ile to możliwe, stosuje się odpowiednie środki w celu zapobieżenia występowaniu nieprawidłowości w przyszłości.
4. Przegląd programów i narzędzi przeprowadzany jest w przypadku zmiany wersji oprogramowania, zmiany systemu operacyjnego, chyba że zmiany te wynikają z aktualizacji automatycznej.

B. Naprawy urządzeń komputerowych z chronionymi danymi osobowymi

1. Naprawy i zmiany w systemie informatycznym przeprowadzane przez serwisanta prowadzone są pod nadzorem w siedzibie ADO - o ile to możliwe - lub poza siedzibą ADO, po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.
3. Jeśli nośnik danych (dysk, dyskietka, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie w niszczarce.

C. Ewidencjonowanie informacji o odbiorcach danych

1. Dla każdej osoby, której dane osobowe przetwarzane są w systemie informatycznym, w systemie powinna zostać odnotowana informacja o udostępnieniach danych odbiorcom, zawierająca informacje, komu, kiedy i w jakim zakresie dane osobowe zostały udostępnione.
2. Szczegółowy sposób oraz formę odnotowania informacji, o których mowa w ust. 1, zawiera dokumentacja techniczna danego systemu informatycznego.

KOPIE ZAPASOWE

A. Cel i zasady tworzenia kopii zapasowych

1. W celu zwiększenia poziomu bezpieczeństwa oraz zapewnienia ciągłości działania jednostki zaleca się regularne tworzenie kopii zapasowe danych.
2. Kopie zapasowe tworzy się wykorzystując narzędzia programowe oraz narzędzia systemu.

B. Procedura tworzenia kopii zapasowych

Kopie zapasowe zbiorów danych wykonywane są zgodnie z harmonogramem przyjętym przez ADO.

C. Nośniki danych wykorzystywane do sporządzenia kopii zapasowych

1. Kopie zapasowe baz danych są nagrywane na zewnętrzne nośniki, takie jak:
1) pamięć USB,
2) CD/DVD,
3) zewnętrzne dyski pamięci.
2. Nośniki zawierające kopie zapasowe należy oznaczać jako "Kopia zapasowa” wraz z podaniem daty sporządzenia.

D. Przechowywanie kopii zapasowych

1. Wszystkie nośniki bez względu na ich rodzaj są zabezpieczane przed nieautoryzowaną zmianą, zniszczeniem i dostępem.
2. Kopie zapasowe przechowuje się w zamykanej szafie w siedzibie ADO.

E. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe

1. Zbiory danych przechowywane są na serwerze/dysku obsługującym system informatyczny ADO. Wszelkie dane przetwarzane w pamięci poszczególnych stacji roboczych oraz komputerów przenośnych są niezwłocznie umieszczane w odpowiednich miejscach na serwerze/dysku, przydzielonych każdemu użytkownikowi.
2. Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną bez uprzedniego zaszyfrowania.
3. Na nośnikach, o których mowa w pkt 2, dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.
4. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na wyznaczonym w tym celu stanowisku komputerowym oraz do oznakowania tego nośnika.
5. Nośniki magnetyczne raz użyte do przetwarzania danych osobowych nie mogą być wykorzystywane do innych celów mimo usunięcia danych i podlegają ochronie w trybie niniejszej Instrukcji.
6. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.

F. Likwidacja nośników zawierających kopie

1. Nośniki, które uległy uszkodzeniu lub zawierają nieaktualne kopie danych, powinny zostać bezzwłocznie zniszczone.
2. W przypadku nośników jednorazowych, takich jak płyty CD-R, DVD-R, likwidacja polega na ich fizycznym zniszczeniu w taki sposób, by nie można było odczytać ich zawartości.
3. Nośniki wielorazowego użytku, takie jak dyski twarde, dyskietki, płyty CD-RW, DVD-RW, można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości.
4. Nośniki wielorazowego użytku nienadające się do ponownego użycia należy zniszczyć fizycznie.
5. Proces niszczenia kopii powinien zostać odnotowany w rejestrze kopii zapasowych.

G. Bezpieczeństwo nośników informacji

1. Zasady ogólne:

1) wszystkie nośniki informacji podlegają właściwej ochronie stosownie do klasyfikacji informacji, na wszystkich etapach ich używania, od momentu zapisu informacji, aż do momentu wycofania z użycia lub fizycznego zniszczenia opisanego w IZSI;
2) za zapewnienie właściwej ochrony nośników informacji odpowiada ich użytkownik;
3) osoby korzystające z nośników informacji powinny być świadome zagrożeń i zobowiązane są do zachowania należytej staranności poprzez zastosowanie obowiązujących środków organizacyjno-technicznych i prawnych opisanych w IZSI;
4) w przypadku wycofywania z użycia nośników informacji zawierających informacje stanowiące tajemnicę, na osobie, której nośnik przekazano do używania, spoczywa obowiązek wykonania procedury opisanej w IZSI.

2. Zasady szczegółowe:

1) urządzenia przenośne oraz nośniki danych wynoszone z siedziby ADO nie powinny być pozostawiane bez nadzoru w miejscach publicznych. Komputery przenośne należy przewozić w służbowych torbach;
2) nie należy pozostawiać bez kontroli dokumentów, nośników danych i sprzętu w miejscach publicznych ani też w samochodach;
3) informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi, a ze względu na działanie silnego pola elektromagnetycznego należy przestrzegać zaleceń producentów dotyczących ochrony sprzętu;
4) wykorzystywanie komputerów przenośnych w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki

minimalizujące ryzyko zapoznania się z danymi przez osoby nieupoważnione. W konsekwencji korzystanie z komputera przenośnego będzie z reguły niedozwolone w restauracjach czy środkach komunikacji publicznej;

5) w domu niedozwolone jest udostępnianie domownikom komputera przenośnego należącego do ADO. Użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym.

POSTĘPOWANIE W PRZYPADKU STWIERDZENIA NARUSZENIA BEZPIECZEŃSTWA

A. Definicja naruszenia bezpieczeństwa systemu

1. Za naruszenie bezpieczeństwa systemu informatycznego uznawany jest każdy stwierdzony fakt oraz uzasadnione podejrzenie, w szczególności:

1) nieuprawnionego ujawnienia danych, udostępnienia;
2) naruszenia hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła);
3) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień;
4) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera/dysku;
5) wykryciu wirusa komputerowego,
6) zauważeniu elektronicznych śladów próby włamania do systemu informatycznego;
7) znacznym spowolnieniu działania systemu informatycznego;
8) podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe;
9) istotnej zmianie położenia sprzętu komputerowego;
10) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf;
11) umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną;
12) uszkodzenie lub zniszczenie danych lub jakiegokolwiek elementu systemu informatycznego;
13) działanie wbrew postanowieniom Instrukcji.

B. Tryb postępowania

1. Każdy użytkownik systemu posiadający informacje o naruszeniu albo uzasadnione podejrzenie naruszenia bezpieczeństwa systemu informatycznego obowiązany jest bezzwłocznie poinformować o danym fakcie ADO.

2. Użytkownik do czasu przybycia na miejsce ADO podejmuje tylko takie czynności, które zmierzają do:

1) zabezpieczenia śladów naruszenia,
2) zapobieżenia dalszym zagrożeniom,
3) powstrzymania skutków naruszenia,
4) ustalenia przyczyny i sprawcy naruszenia ochrony,
5) rozważenia wstrzymania bieżącej pracy w celu zabezpieczenia miejsca zdarzenia,
6) przygotowania opisu incydentu.

3. Pracownik nie opuszcza bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia ADO lub osoby przez niego wskazanej.

4. ADO po otrzymaniu zawiadomienia, o którym mowa w pkt 1, powinien niezwłocznie:

1) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
2) podjąć działania chroniące system przed ponownym naruszeniem.

5. W przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego.

6. ADO może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.

7. W razie odtwarzania danych z kopii zapasowych ADO obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu (dotyczy to zwłaszcza przypadków infekcji wirusowej).

8. ADO podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego bądź zastosowaniu środków ochrony fizycznej.

POSTANOWIENIA KOŃCOWE

A. Stosowanie Instrukcji

1. Instrukcja jest dokumentem wewnętrznym jednostki i jest objęta obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.
2. W sprawach nieokreślonych niniejszą Instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
3. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą Instrukcją oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.